COFC

OIPE JC143 AUG 17 2005 PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of: Jordan J. Glogau	)	Group Art No.: 2132
	)	Examiner: Minh Dinh
Serial No.: 09/485,759	)	Patent No.: 6,912,658 B1
Filed: February 15, 2000	)	Issued: June 28, 2005
HIDING OF ENCRYPTED DATA	)	August 15, 2005
	)	Attorney Docket: 3220-60866

REQUEST FOR CERTIFICATE OF CORRECTION OF PATENT
FOR PTO MISTAKE UNDER 37 CFR § 1.322(a)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Attention: Certificate of Correction Branch

Certificate
AUG 19 2005
of Correction

Sir:

A Certificate of Correction under Rule 1.322 in the above-identified patent is respectfully requested in accordance with the enclosed copies of form PTO/SB/44.

The Letters Patent No. 6,912,658 as issued on June 28, 2005 incorrectly lists claim 5. Original claim 20 was amended and allowed on January 21, 2005 as claim 5 of the above-identified patent. The patentee requests that all records be corrected to show the correct version of claim 5 as amended on January 21, 2005.

Certificate of Mailing (37 C.F.R. §1.8(a))

I hereby certify that, on the date shown below, this correspondence is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 the date indicated below.

August 15, 2005 By: _____

AUG 22 2005

The Commissioner is hereby authorized to charge any fees associated with this Certificate of Correction to Deposit Account No. 10-0435 with reference to our Matter Number 3220-60866. A duplicate copy of this letter is attached for that purpose.

Respectfully submitted,

Jeffrey A. Michael
Reg. No. 37,394
Barnes & Thornburg
11 South Meridian Street
Indianapolis, Indiana 46204-3335
Tel.: (317) 231-7382
Fax: (317) 231-7433

AUG 2 2 2005

PTO/SB/44 (04-05)
Approved for use through 04/30/2007. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,912,658 B1

APPLICATION NO.: 09/485,759

ISSUE DATE : June 28, 2005

INVENTOR(S) : Glogau et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Please correct claim 5 of the specification (column 9, lines 16-23 through column 10, lines 1-2) to read:

A method of data hiding comprising the steps of:
embedding an encrypted message into a first portion of a carrier signal; and
embedding message extraction information into a second portion of the carrier signal for extracting the encrypted message from the first portion of the carrier signal, wherein the step of embedding an encrypted message includes performing an exclusive-OR of the encrypted message with the first portion of the carrier signal.

MAILING ADDRESS OF SENDER (Please do not use customer number below):

Jeffrey A. Michael / Barnes & Thornburg
11. S. Meridian Street
Indianapolis, IN 46204 (317) 231-7382

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

AUG 2 2 2005

BEST AVAILABLE COPY

Issue Classification	Application No.	Applicant(s)	
	09/485,759	GLOGAU ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

ISSUE CLASSIFICATION

ORIGINAL					CROSS REFERENCE(S)							
CLASS			SUBCLASS		CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)						
713			176		380	43						
INTERNATIONAL CLASSIFICATION												
H	0	4	L	9/00								
				/								
				/								
				/								
				/								

MD
Minh Dinh 1/21/2005
(Assistant Examiner) (Date)

Kim Watson-Saunders 1/25/05
(Legal Instruments Examiner) (Date)

1/24/05
GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100
(Primary Examiner) (Date)

Total Claims Allowed: 8

O.G. Print Claim(s)	O.G. Print Fig.
1	2

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		31		61		91		121		151		181
	2		32		62		92		122		152		182
	3		33		63		93		123		153		183
1	4		34		64		94		124		154		184
2	5		35		65		95		125		155		185
	6		36		66		96		126		156		186
	7		37		67		97		127		157		187
	8		38		68		98		128		158		188
	9		39		69		99		129		159		189
	10		40		70		100		130		160		190
	11		41		71		101		131		161		191
	12		42		72		102		132		162		192
	13		43		73		103		133		163		193
	14		44		74		104		134		164		194
	15		45		75		105		135		165		195
	16		46		76		106		136		166		196
3	17		47		77		107		137		167		197
4	18		48		78		108		138		168		198
	19		49		79		109		139		169		199
5	20		50		80		110		140		170		200
6	21		51		81		111		141		171		201
7	22		52		82		112		142		172		202
	23		53		83		113		143		173		203
	24		54		84		114		144		174		204
	25		55		85		115		145		175		205
	26		56		86		116		146		176		206
	27		57		87		117		147		177		207
	28		58		88		118		148		178		208
8	29		59		89		119		149		179		209
	30		60		90		120		150		180		210

OIPE JC143 AUG 17 2005 PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Art Unit:	2132
Confirmation No.:	2173
Application No.:	09/485,759
Title:	HIDING OF ENCRYPTED DATA
Inventor:	Jordan J. Gloat et al.
Filing Date:	February 15, 2000
Attorney Docket No.:	3220-60866
Examiner:	Minh Dinh

Certificate Under 37 CFR 1.8(a)
I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office (Division), fax number (571)273-3802
on JANUARY 21, 2005
Jeffrey A. Michael
(Signature)
Jeffrey A. Michael
(Printed Name)

RESPONSE FOLLOWING TELEPHONE INTERVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to a telephone interview between Examiner Minh Dinh and the undersigned on January 20, 2005, please consider the following. The commissioner is authorized to charge any fees which may be due to Deposit Account 10-0435, but not to include any payment of issue fees.

Amendments to the Claims begin on page 2 of this paper.

Remarks begin on page 4 of this paper.

Amendments to the Claims:

14. (canceled)

15. (canceled)

16. (canceled)

17. (currently amended) A method of data hiding comprising the steps of:

providing an encryption key;

generating an encryption sequence based on the encryption key;

providing a carrier signal that conveys information unrelated to the encryption key;

embedding the encryption sequence into the carrier signal,

transmitting the carrier signal including the embedded encryption sequence to a receiving location,

extracting the encryption sequence from the composite signal at the receiving location, and

deciphering the encryption sequence to obtain the encryption key at the receiving location.

19. (canceled)

20. (currently amended) A method of data hiding comprising the steps of:

embedding an encrypted message into a first portion of a carrier signal; and

embedding message extraction information into a second portion of the carrier signal for extracting the encrypted message from the first portion of the carrier signal, ~~The method of claim 19,~~ wherein the step of embedding an encrypted message includes performing an exclusive-OR of the encrypted message with the first portion of the carrier signal.

26. (canceled)

29. (currently amended) A data hiding apparatus comprising:

an encryption sequence generator configured to generate an encryption sequence based on an encrypting key;

an encrypted message generator configured to generate an encrypted message based on the encryption sequence and an input message; and

an encrypted message embedder configured to embed the encrypted message into a carrier signal by replacing a first LSB plane of ~~the~~ a digital image with information based on a second LSB plane of the digital image and performing an exclusive-OR of the encrypted message with the second LSB plane of the digital image.

REMARKS

Reconsideration of the above-identified patent application, as amended, is respectfully requested.

In a telephone interview conducted between Examiner Dinh and the undersigned on January 20, 2005, it was agreed that claims 14-16, 19 and 26 would be canceled, that claim 20 would be amended to include all of the limitations of canceled claim 19, and that claim 29 would be amended to address an antecedent basis issue. Accordingly, claims 14-16, 19 and 26 have been canceled herein. Claims 20 and 29 have been amended as suggested by the Examiner. Claim 17 has also been amended herein to correct a punctuation error.

Claims 4-5, 17-18, 20-22 and 29 are believed to be in condition for allowance, and such action is solicited. The Examiner is cordially invited to contact the undersigned by telephone to discuss any further unresolved matters.

Respectfully submitted,

Jeffrey A. Michael
Registration No. 37,394
Barnes & Thornburg
11 South Meridian Street
Indianapolis, Indiana 46204-3335
Telephone: (317) 231-7382
Fax: (317) 231-7433

US006912658B1

(12) **United States Patent**
Glogau et al.

(10) **Patent No.: US 6,912,658 B1**
(45) **Date of Patent: Jun. 28, 2005**

(54) **HIDING OF ENCRYPTED DATA**

(75) Inventors: **Jordan J. Glogau**, Nanuet, NY (US); **Edward J. Delp, III**, West Lafayette, IN (US); **Raymond B. Wolfgang**, Exton, PA (US); **Eugene Ted Lin**, West Lafayette, IN (US)

(73) Assignee: **Purdue Research Foundation**, West Lafayette, IN (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/485,759**

(22) PCT Filed: **Aug. 21, 1998**

(86) PCT No.: **PCT/US98/17321**

§ 371 (c)(1),
(2), (4) Date: **Feb. 15, 2000**

(87) PCT Pub. No.: **WO99/11020**

PCT Pub. Date: **Mar. 4, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/056,724, filed on Aug. 22, 1997.

(51) **Int. Cl.**[7] **H04L 9/00**
(52) **U.S. Cl.** **713/176**; 380/43
(58) **Field of Search** 380/43, 54, 253–254, 380/232, 239, 250; 713/176–179

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,471,164 A	*	9/1984	Henry	380/30
5,195,136 A		3/1993	Hardy et al.	
5,751,813 A	*	5/1998	Dorenbos	713/153
5,912,972 A	*	6/1999	Barton	713/176
5,970,140 A	*	10/1999	Sandford et al.	380/205

FOREIGN PATENT DOCUMENTS

EP 0 359 325 A1 9/1989

OTHER PUBLICATIONS

Schneier, B., Applied Cryptography, 1996, John Wiley & Sons, Inc., 2nd Edition, pp. 31–32.*
Schyndell, et al., A Digital Watermark, 1994, IEEE.*
Tirkel, et al., Image Watermarking—A Spread Spectrum Application.*
Bruce Schneier, Applied Cryptography, second edition, p. 185–186.*
"A Unified Coding Method of Dithered Image and Text Data Using Micropatterns", Yasuhiro Nakamura and Kineo Matsui, Electronics and Communications in Japan, Part 1, vol. 72, No. 4, 1989, pps. 50–56.
"Secure Spread Spectrum Watermarking for Multimedia", Ingemar J. Cox, Joe Kilian, F. Thomason Leighton, and Talal Shamoon, IEEE Transactions on Image Processing, vol. 6, No. 12, Dec. 1997, pps. 1673–1687.
"Digital Image Watermarking Using Visual Models", Christine I. Podilchuk and Wenjun Zeng, SPIE, vol. 3016, 1997, pps. 100–111.

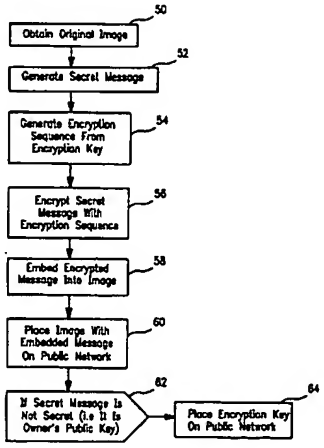
* cited by examiner

Primary Examiner—Gregory Morse
Assistant Examiner—Minh Dinh
(74) *Attorney, Agent, or Firm*—Barnes & Thornburg

(57) **ABSTRACT**

A method of data hiding includes providing a message (**68**), providing an encrypting sequence (**86**), and generating an encrypted message (**72**) based on the message and the encrypting sequence. A carrier signal (**66**) that conveys information unrelated to the encrypted message is provided, and the encrypted message is embedded (**78**) into the carrier signal by performing an exclusive-OR of the encrypted message with a first portion of the carrier signal.

8 Claims, 4 Drawing Sheets



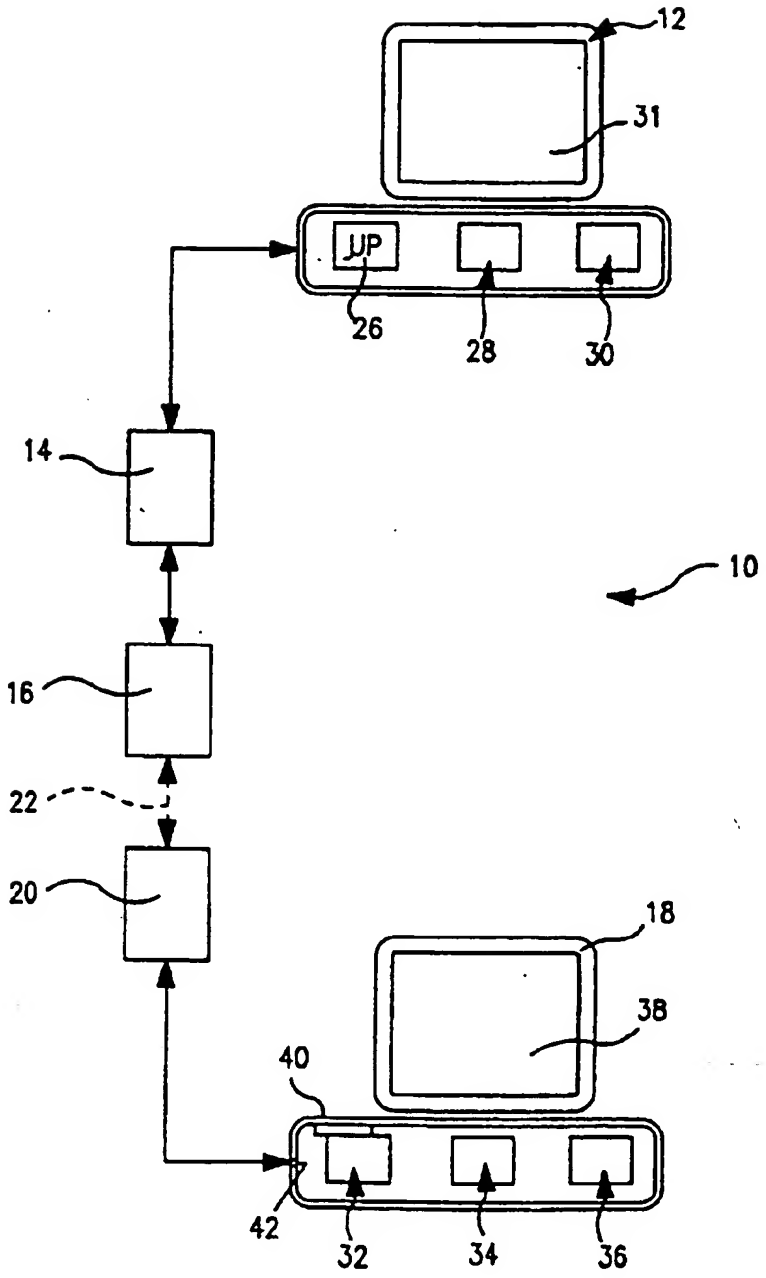


FIG. 1

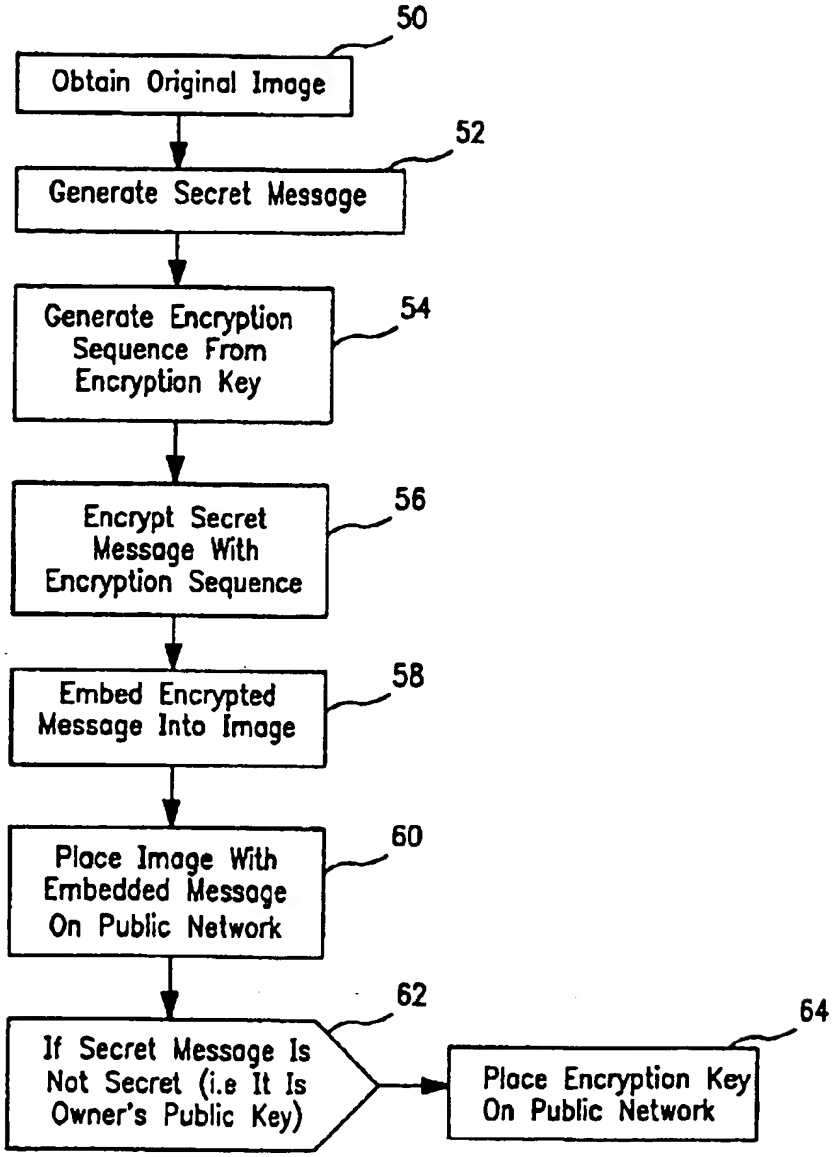

50
Obtain Original Image
52
Generate Secret Message
54
Generate Encryption Sequence From Encryption Key
56
Encrypt Secret Message With Encryption Sequence
58
Embed Encrypted Message Into Image
60
Place Image With Embedded Message On Public Network
62
If Secret Message Is Not Secret (i.e It Is Owner's Public Key)
64
Place Encryption Key On Public Network

FIG. 2

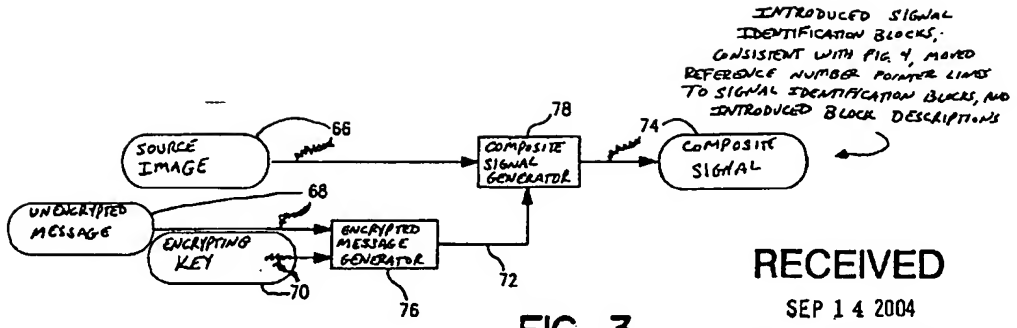


FIG. 3

RECEIVED
SEP 14 2004
Technology Center 2100

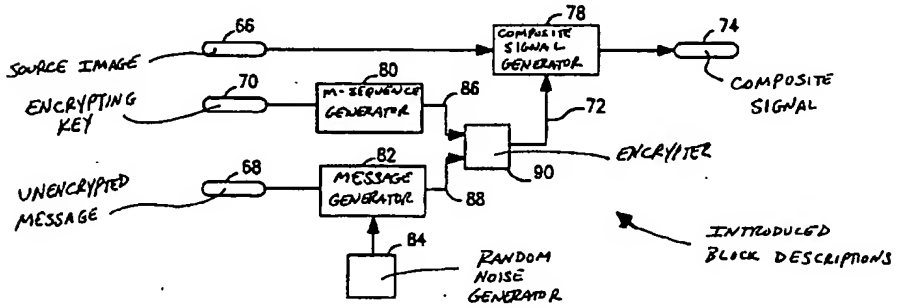


FIG. 4

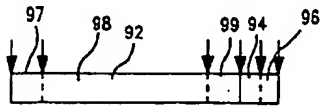


FIG. 5

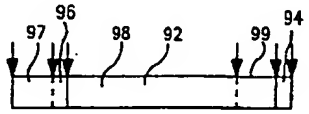


FIG. 6

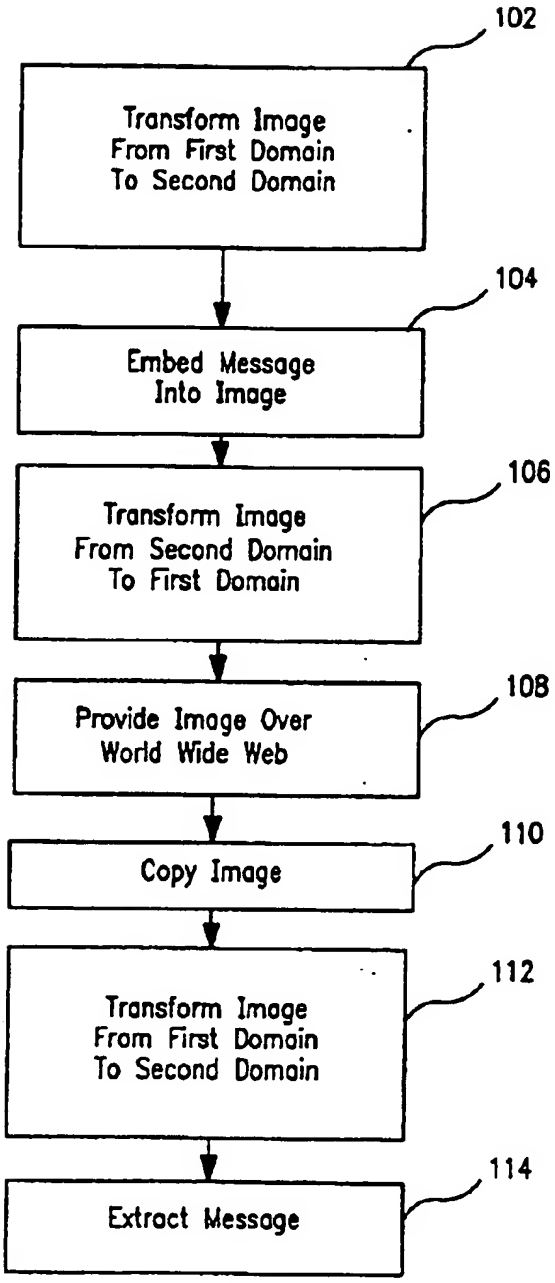

102
Transform Image From First Domain To Second Domain
104
Embed Message Into Image
106
Transform Image From Second Domain To First Domain
108
Provide Image Over World Wide Web
110
Copy Image
112
Transform Image From First Domain To Second Domain
114
Extract Message

FIG. 7

HIDING OF ENCRYPTED DATA

CROSS-REFERENCES TO RELATED APPLICATIONS

This application is a U.S. national application of international application serial No. PCT/US98/17321 filed Aug. 21, 1998, which claims priority to U.S. provisional application Ser. No. 60/056,724 filed Aug. 22, 1997.

FIELD OF THE INVENTION

The present invention relates to methods and apparatus for hiding data within a digital signal, and particularly for concealing information within multimedia signals such as digital image, audio, or video signals. More particularly, the present invention relates to methods and apparatus for embedding and retrieving information into and out of a digital signal used in multimedia applications while minimizing the effect on the multimedia application of the digital signal.

BACKGROUND AND SUMMARY OF THE INVENTION

The art of concealing information has existed for millennia and is one to which computers have been readily adapted. It is known, for example, to use computers for encrypting data using various symmetric and asymmetric cryptographic schemes such as the Data Encryption Standard (DES) and RSA encryption, and cryptographic software packages such as PGP (Pretty Good Privacy). Another technique for concealing information for which computers are used is data hiding or steganography, in which the existence of certain information is concealed within a carrier communication. In contrast to cryptography, where it is a goal to make a message undecipherable regardless of its detection, with steganography it is a goal to hide the very existence of the hidden message. An example of a known steganography technique using computers is to embed a digital watermark into a digital image.

According to the present invention, a method of hiding data is provided. A message to be hidden and an encrypting sequence are provided along with a carrier signal that conveys information (unrelated to the message). An encrypted message is generated based on the message and the encrypting sequence. The encrypted message is embedded into the carrier signal by performing an exclusive-OR of the encrypted message with a first portion of the carrier signal.

In preferred embodiments, the carrier signal is a digital image, and the first portion of-the carrier signal is an LSB plane of the digital image. The digital image has a plurality of color planes, the first portion of the carrier signal is an LSB plane of a first color plane, and the second portion of the carrier signal is an LSB plane of a second color plane.

According to another aspect of the invention, the carrier signal is transmitted to a receiving location. The encrypted message is extracted and from the carrier signal and deciphered at the receiving location. In preferred embodiments, the encrypted sequence is generated based on an encrypting key. The encrypted message is generated by performing an exclusive-OR of the message with the encrypting sequence.

According to yet another aspect of the invention, a method of data hiding is provided in which an encryption key and a carrier signal that conveys information unrelated to the encryption key are supplied. An encryption sequence based on the encryption key is generated. The encryption sequence is embedded into the carrier signal.

In preferred embodiments, the encryption key is a public key for an asymmetric encryption algorithm. The carrier signal can be a signal such as a digital image, digital audio, or digital video. The encryption sequence is substantially random, and can be generated based on a linear feedback shift register. The encryption sequence is embedded into the carrier signal by performing an exclusive-OR of the encryption sequence with a portion of the carrier signal.

According to other aspects of the invention, the carrier signal including the embedded encryption sequence is transmitted to a receiving location. The encryption sequence is extracted from the composite signal at the receiving location. The encryption sequence is decrypted to obtain the encryption key. The encryption key is used to generate an encrypted message at the receiving location, and the encrypted message is transmitted from the receiving location.

According to yet another aspect of the invention, a method of data hiding is provided. An encrypted message is embedded into a first portion of a carrier signal and message extraction information is embedded into a second portion of the carrier signal for extracting the encrypted message from the first portion of the carrier signal.

In preferred embodiments, the encrypted message is embedded by performing an exclusive-OR of the encrypted message with the first portion of the carrier signal. The message extraction information is embedded by performing an exclusive-OR of the first portion of the carrier signal with the second portion of the carrier signal. The first and second portions of the carrier signal can be first and second bit-planes of a digital image.

According to still another aspect of the invention, a method of exchanging data hidden in a carrier signal is provided. A signal including hidden data is generated by transforming a carrier signal from a first domain into a second domain. A message is embedded into the carrier signal in the second domain. The carrier signal is transformed back from the second domain to the first domain. The signal including hidden data is sent to a receiving location. The message is obtained from the signal including hidden data at the receiving location by transforming the signal including hidden data into the second domain and extracting the message.

In preferred embodiments, the message is encrypted prior to generating the signal including hidden data. The message is decrypted after obtaining the message from the signal including hidden data.

According to still yet another aspect of the invention, a data hiding apparatus is provided. An encryption sequence generator generates an encryption sequence based on an encrypting key. An encrypted message generator generates an encrypted message based on the encryption sequence and an input message. An encrypted message embedder embeds the encrypted message into a carrier signal.

In preferred embodiments, the encryption sequence generator generates a substantially random encryption sequence. The encrypted message embedder performs an exclusive-OR of the encrypted message with a portion of the carrier signal. The encrypted message embedder replaces a first LSB plane of a digital image with information based on a second LSB plane of the digital image and performs an exclusive-OR of-the encrypted message with the second LSB plane of the digital image. The encrypted message generator performs an exclusive-OR of the input message with the encrypting sequence to generate the encrypted message.

Additional features of the invention will become apparent to those skilled in the art upon consideration of the following detailed description of the preferred embodiments exemplifying the best mode of carrying out the invention as presently perceived.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of two computer systems connected over a network, each computer system configured with a processor and memory for implementing embodiments of the present invention;

FIG. **2** is a flow chart showing a method according to the present invention for hiding data within an image for transmission over a network;

FIG. **3** is a high level block diagram showing a technique for embedding encrypted information into a carrier signal;

FIG. **4** is a more detailed block diagram similar to FIG. **3** showing a similar, more specific technique for embedding encrypted information into a carrier signal;

FIG. **5** is a stylized representation of a message format containing embedded, hidden information;

FIG. **6** is a stylized representation similar to FIG. **5** of an alternative message format; and

FIG. **7** is a flow chart showing an alternative method according to the present invention for hiding data within an image for transmission over a network.

DETAILED DESCRIPTION OF THE ILLUSTRATIVE EMBODIMENTS

The present invention lends itself to implementation in a conventional computer network **10** as shown in FIG. **1**. Computer network **10** illustratively includes computer systems **12, 18** connected through a series of network communication devices **14, 16, 20** (e.g., modems, transceivers, etc.) for communication over a network **22** such as the standard telephone lines, or the Internet or World Wide Web. Computer systems **12, 18** are illustratively personal computers and each includes basic elements such as a processor **26, 32**, memory **28, 34**, storage device **30, 36**, and display **31, 38**. Computer systems **12, 18** can also include optional peripheral devices such as removable storage device **40** (e.g., a CD-ROM or 3½ inch disk drive).

An exemplary method of data hiding according to the present invention that is suitable for carrying out on computer network **10** is shown in FIG. **2**. Although the present invention is disclosed in the context of certain embodiments discussing digital images, other digital signals, such as digital audio or video signals, are also within the scope of the invention.

According to the method of FIG. **2**, an image is used to transport and exchange data that is embedded in the image itself and that cannot be perceived by the human eye. An appropriate analogy is that the image acts as an envelope, with the embedded data transmitted with the image being equivalent to a letter contained within the envelope. Conventional encryption such as PGP or RSA is used to enhance security of the embedded data. The security is improved because the encrypted data is hidden within the image and therefore cannot be recognized as such. This allows for secure data communication and exchange over an insecure transmission channel.

In step **50** an original digital image is obtained. A secret message that is desired to be embedded into the image is generated in step **52**. A message encrypting key is used in step **54** to generate an encryption sequence. The message encrypting key can be a seed value for use in generating an m-sequence from a linear feedback shift register as discussed in more detail below, although it is understood that any suitable message encrypting algorithm can be used. As also discussed below, the message encrypting key will ultimately be used by the recipient of the image embedded with the secret message.

In step **56** the secret message from step **52** is encrypted with the encryption sequence from step **54** to create an encrypted message. The encrypted message is then embedded into the image in step **58**. There are many methods to embed the encrypted message into the image such as the method discussed below, but, again, it is understood that other suitable methods can be used.

The image with the embedded message is then made available such as on a public network as shown in step **60**. Finally, if the secret message from step **52** is actually information that is not desired to be kept secret, such as a public key for an asymmetric encryption algorithm, then the encryption key from step **54** is also made available on the public network as shown in steps **62, 64**. This allows for third parties to extract the message from the image. Thus, for example, the message can be a public encryption key that is hidden within the image but that is readily available to a party that has knowledge of the fact that the hidden message exists. This provides a convenient way of exchanging information, such as allowing an individual to make a public encryption key available over the World Wide Web by posting it within an image on a Web site, while still concealing the information from the casual observer.

It is useful at this point to provide some preliminary definitions before discussing a specific implementation of the method of FIG. **2**. The symbol $\oplus$ denotes a bit exclusive-OR function (equivalently, modulo-2 addition). Table 1 illustrates the exclusive-OR function:

TABLE 1

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

A digital image is typically represented with a two dimensional array of pixel values. If A is the array of pixel values, then A(x,y) denotes the pixel value in the x-th column of the y-th row of the array. Each index x,y begins at zero, and by convention the origin is at the upper-left corner with positive coordinates going rightwards and downwards, although this convention is somewhat arbitrary.

For labeling purposes, it will be assumed that the digital image is a 24-bit RGB image with pixel values ordered as shown in Table 2: xx

TABLE 2

MSB															LSB							
Red								Green								Blue							
23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
R7	R6	R5	R4	R3	R2	R1	R0	G7	G6	G5	G4	G3	G2	G1	G0	B7	B6	B5	B4	B3	B2	B1	B0

Thus, bits **16–23** refer to the red component, bits **8–15** refer to the green component, and bits **0–7** refer to the blue component for any given pixel value. For example, $I_{G0}(x,y)$ refers to the least-significant bit of the green component of the (x,y)-pixel in the image I. Since bit G0 is equivalent to bit **8**, $I_{G0}(x,y)$ is equivalent to $I_8(x,y)$. As with the array convention, this labeling convention is somewhat arbitrary.

An m-sequence is a pseudo-random sequence of binary digits (bits). m-sequences have good statistical properties and can be generated by linear feedback shift registers (configured appropriately as is known in the art). Knowing the size (number of bits), structure (the feedback configuration), and initial fill (the initial contents of each bit) of the shift register allows the reconstruction of the entire m-sequence. The m-sequences here illustratively are generated by a 96-bit m-sequence generator. If the structure and size of the shift register are known (as would be the case with this embodiment), and if a consecutive portion of the m-sequence equal to twice the shift register size is also known, the initial fill used to generate the sequence can be determined. In this embodiment the initial fill is used as the key that generates the m-sequence. In this way, the key can be determined from the sequence itself by techniques known to those skilled in cryptography.

When embedding a message into a carrier signal, the order in which pixel operations are performed may be an important consideration. A sequence function z(i) is defined to provide a one-to-one mapping from i->(x,y), where i is an ordinal number and (x,y) refers to coordinate values in an image. The ordinal i ranges from zero to N-1, where N is the total number of pixels in the image. Given a sequence function z(i), one can compute z(**0**), z(**1**), z(**2**), etc., to obtain a sequence of pixel coordinates (x_1,y_1), (x_2,y_2), etc. As an example, z(i)=(i mod ImageWidth, ⌊i/ImageWidth⌋) denotes a sequence beginning at the origin and proceeding in a row-by-row fashion.

Given these preliminary definitions, an implementation corresponding to the illustrative method of FIG. **2** of embedding a message into an image is shown by the block diagram in FIG. **3**. Input signals are a source image **66** (obtained in step **50**), an unencrypted message **68** (generated in step **52**), and an encrypting key **70** (used in step **54**). Message **68** and encrypting key **70** are processed by an encrypted message generator **76** to create an encrypted message signal **72**. Encrypted message **72** is an input along with source image **66** into composite signal generator **78**, which creates a composite signal **74** containing source image signal **66** embedded with encrypted message **72**.

Composite signal generator **78** illustratively embeds encrypted message **72** into the least-significant bit in the green plane $I_{G0}(x,y)$ of source image **66** to create a new least-significant green bit-plane $I'_{G0}(x,y)$ of composite signal **74**. In order subsequently to extract encrypted message **72** from composite signal **74** (I') it will be necessary to know the original values of $I_{G0}(x,y)$ from source image **66**. This can of course easily be accomplished by making the original, unmodified image signal **66** available. Composite signal generator **78**, however, eliminates the requirement of using original image signal **66** by encoding the original $I_{G0}(x,y)$ into the least-significant red bit-plane $I'_{R0}(x,y)$ of composite signal **74** as discussed below. Thus, in order to extract the embedded encrypted message **72**, only composite signal **74** and the encrypting key **70** are needed.

In order to use the method of FIGS. **2** and **3** both a sender and receiver of composite signal **74** will need an m-bit shift register with identical feedback configurations and a well-defined ordering function z(i) for any arbitrary image. The following steps describe the generation of the composite signal **74** (also referred to as public image I') from original signal **66** (also referred to as original image I), unencrypted message **68** (illustratively a public encryption key, also referred to as K_{PUB}), and encrypting key **70** (also referred to as K_I). As intimated above, encrypting key **70** (K_I) is the initial fill of the m-sequence generator.

In order to generate I', I' is initially set to be an exact copy of I. I' is then traversed in order z(i) and the red and green least-significant bit planes are set to:

$$I'_{R0}(z(i))=I'_{G0}(z(i))\oplus m\text{-seq}(2i)$$

$$I'_{G0}(z(i))=K_{PUB}(i)\oplus I'_{G0}(z(i))\oplus m\text{-seq}(2i+1)$$

where $K_{PUB}(i)$ refers to the I-th bit of K_{PUB}, and m-seq(j) refers to the j-th bit in the m-sequence using K_I as the initial fill. With these two equations, information on portion **2** of the image (the green LSB plane) is first placed in portion **1** of the image (the red LSB plane). Then, the message is embedded in portion **2**.

To recover K_{PUB} it is only necessary to have the composite signal or public image I' and the encrypting key K_I. For each pixel in I' and in the order z(i), the first step is to extract $I_{G0}^*(z(i))$ by using the least-significant red bit plane and the m-sequence:

$$I_{G0}^*(z(i))=I'_{R0}(z(i))\oplus m\text{-seq}(2i)$$

$I_{G0}^*(z(i))$ is identical to $I_{G0}(z(i))$ if there are no errors in I'. Then the i-th bit of $K_{PUB}(i)$ is computed by using $I_{G0}^*(z(i))$:

$$K_{PUB}^*(i)=I'_{G0}(z(i))\oplus I_{G0}^*(z(i))\oplus m\text{-seq}(2i+1)$$

Thus, given K_I, it is possible to reconstruct the same m-sequence used to generate I'. Thus, if no errors occur K_{PUB}^* should be identical to K_{PUB}. Thus, the method of the invention provides for including within the image both the message that is embedded or encrypted in the image as well as the information needed to extract or decrypt the message from the image.

A more specific method corresponding to an implementation of the method of FIGS. **2** and **3** is shown FIG. **4**. The same input signals are used, that is, source image **66** (I), message **68** (here, Q instead of K_{PUB}), and encrypting key **70** (K_I) are used. The primary refinement in the method of FIG. **4** as compared with FIG. **3** is an encoding process to handle varying length messages **68**.

Message **68**, which in the example of FIG. **3** was a public encryption key for use in an asymmetric cryptography

system, can more generally simply be a collection of bits intended to be encrypted and is referred to here as Q. The length (i.e., the total number of bits) of Q is denoted |Q|. The i-th bit of the message Q is denoted Q(i), where the bits are numbered from 0 to |Q|−1.

Message **68** (Q) is an input signal to message generator **82** which has as a second input the output from a random noise generator **84**. Random noise generator **84** illustratively is also a 96-bit m-sequence generator using an initial fill of a computer system time value, although other suitable random signal generators can be used. Encrypting key **70** (K_r) is an input signal (initial fill) to an m-sequence generator **80** that illustratively is the same as random noise generator **84**, which then generates as an output an encrypting sequence **86**.

Unless the message **68** (Q) will always be the same length (in bits) and that length is the number of pixels in the source image, it will not be possible to embed Q directly onto source image **66** (I). It is therefore necessary to encode additional information that will enable subsequent extraction of messages Q of varying sizes from composite signal **74** (I'). Thus, the message **88** to be encoded onto image **66** (I) is generated by message generator **82** with special properties and is denoted Q' to show that it is derived from Q.

Q' has the following properties. For any given source image I, regardless of what message Q is being encoded, the size of a message Q' is the same as the total number of pixels in image I (that is, |Q'|=# pixels in I). The bits of message Q' are labeled according to standard convention, that is, the first bit (or the left-most bit if Q' is viewed as an ordered bit stream from left to right as shown in FIG. **5**) is numbered zero. Thus the bits of Q' are numbered from zero to |Q'|−1.

The structure of Q' is shown in FIG. **5**. All bits except the last sixty-four form a data area **92**. The last sixty-four bits consist of two thirty-two bit words (StartPos and Length, in that order), which form a Trailer. Data area **92** includes data bits **98** that correspond to the message Q itself, and random bits **97**, **99** that help hide the location of Q (bits **98**) within Q'. As part of the encoding process, message generator **82** computes the length of message Q and stores its value in the final 32 bits **94** of the Trailer. The value of the length is not directly encoded and instead a value congruent (actual length modulo Data Area size) is placed in the 32-bit word. It is trivial to recover the length from this encoded value.

Starting position **94** describes the location within data area **92** where the bits of the message Q reside. Message generator **82** randomly chooses a place **98** to store Q and populates all other bits of unused portions **97**, **99** in data area **92** with random noise generated by random noise generator **84**. Thus, Q can be anywhere in data area **92**. Including noise for portions **97**, **99** of data area **92** unused by message Q improves security of data embedded within I because the noise increases the difficulty of recognizing the existence or location of Q within the data area.

The encoding of each bit of message Q' is encoded onto image I on a one-bit per one-pixel basis using an exclusive-OR as discussed above for the method of FIG. **3**. First, the output of m-sequence generator **80** (with K_r as a seed value) is used to encrypt Q' in encrypter **90**. Next, the encrypted Q' is embedded onto the LSB green plane I_{G0}. Encrypted message Q is subsequently extracted from Q' by locating its starting position and length from the trailer. The extracted Q is then decoded as discussed above.

Further implementation steps can be taken to increase security for message Q'. Random number generator **84** and m-sequence generator **80** can be different. Even if both use 96-bit m-sequence generators, this can be achieved simply by changing the feedback coefficients. Moreover, the message length **94** in the trailer can be relocated to data area **92** as shown in FIG. **6**. This relocation will limit the ability of an attacker to take advantage of a known size of message Q.

Another way to provide for security of data hidden within a carrier image is shown by the method of FIG. **7**. In step **102** the carrier image is transformed from a first domain to a second domain. For example, a typical RGB image that is considered to be represented in a spatial domain can be transformed using a discrete cosine transform A message is then embedded into the transformed carrier image in step **104**, using any appropriate technique for embedding a message onto a carrier signal. An example of a transformed image into which a message can be embedded would be a JPEG image. If desired, the message can also be pre-encrypted before being embedded into the transformed image to further improve security. The image is then transformed back into the first domain in step **106** and made available for access by third parties in step **108**.

For a third party to extract the message the steps are essentially reversed. First the image is copied by the third party in step **110**, and it is then transformed into the second domain in step **112** using the same transform performed in step **106**. Finally, the message is extracted in step **114**, again, using any appropriate technique that corresponds to the technique used in step **104** for originally embedding the message. If the message was pre-encrypted then another decryption step (not shown) will be necessary.

Encrypted messages relying on the use of encryption keys are used in the methods discussed above. For example, if a pre-encrypted message is embedded into an image, then the recipient will need a key to decrypt the message. A technique for providing for secure exchanges of encrypted data such as encryption keys that is known in the art is the use of a trusted third party. The trusted third party essentially acts as a secure broker in exchanging data between two other parties. It is within the scope of this invention to exchange information, such as encryption keys, by use of a trusted third party.

Although the invention has been described in detail with reference to certain illustrated embodiments, variations and modifications exist within the scope and spirit of the present invention as described and defined in the following claims.

What is claimed is:

1. A method of data hiding comprising the steps of:

providing a message;

generating an encrypting sequence based on an encrypting key;

generating an encrypted message based on the message and the encrypting sequence;

providing a carrier signal that conveys information unrelated to the encrypted message;

embedding the encrypted message into the carrier signal by performing an exclusive-OR of the encrypted message with a first portion of the carrier signal; and

embedding the first portion of the carrier signal into a second portion of the carrier signal.

2. The method of claim **1**, wherein the carrier signal is a digital image having a plurality of color planes, the first portion of the carrier signal is an LSB plane of a first color plane, and the second portion of the carrier signal is an LSB plane of a second color plane.

3. A method of data hiding comprising the steps of:

providing an encryption key;

generating an encryption sequence based on the encryption key;

providing a carrier signal that conveys information unrelated to the encryption key;

embedding the encryption sequence into the carrier signal,

transmitting the carrier signal including the embedded encryption sequence to a receiving location,

extracting the encryption sequence from the composite signal at the receiving location, and

deciphering the encryption sequence to obtain the encryption key at the receiving location.

4. The method of claim 3, further comprising the steps of encrypting a message using the encryption key to generate an encrypted message at the receiving location and transmitting the encrypted message from the receiving location.

5. A method of data hiding comprising the steps of:

providing a carrier signal that conveys information unrelated to the encryption key;

embedding the encryption sequence into the carrier signal transmitting the carrier signal including the embedded encryption sequence to a receiving location,

extracting the encryption sequence from the composite signal at the receiving location, and

deciphering the encryption sequence to obtain the encryption key at the receiving location.

6. The method of claim 5, wherein the step of embedding message extraction information includes performing an exclusive-OR of the first portion of the carrier signal with the second portion of the carrier signal.

7. The method of claim 6, wherein the first and second portions of the carrier signal are first and second bit-planes of a digital image.

8. A data hiding apparatus comprising:

an encryption sequence generator configured to generate an encryption sequence based on an encrypting key;

an encrypted message generator configured to generate an encrypted message based on the encryption sequence and an input message; and

an encrypted message embedder configured to embed the encrypted message into a carrier signal by replacing a first LSB plane of a digital image with information based on a second LSB plane of the digital image and performing an exclusive-OR of the encrypted message with the second LSB plane of the digital image.

* * * * *